安全漏洞通告

CVE-2021-21087: Adobe ColdFusion 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-03-23

报告信息

报告名称	CVE-2021-21087: Adobe ColdFusion 远程代码执行漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-032301
报告版本	1	**报告日期**	2021-03-23
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-03-23	360CERT	360CERT	撰写报告

目录

一、 漏洞档案 1
二、 漏洞简述 2
三、 漏洞评级 3
四、 漏洞详情 4
五、 漏洞列表 5
六、 安全建议 6
(一) 通用修补方案 6
七、 参考链接 7
附录 A 报告风险等级说明 8
附录 B 影响面说明 10
附录 C 360 内部评分体系 11

一、 漏洞档案

漏洞类型	命令执行
CVE 编号	CVE-2021-21087
相关厂商	adobe
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案
漏洞发布时间	2021-03-23
报告生成时间	2021-03-23

二、 漏洞简述

2021 年 03 月 23 日，360CERT 监测发现 Adobe 官方发布了 Adobe ColdFusion 的风险通告，漏洞编号为 CVE-2021-21087，漏洞等级：严重，漏洞评分：9.8。

Adobe ColdFusion 是一个商用的快速应用程序开发平台，ColdFusion 经常用在数据驱动的网站及内部网的开发上，但也可以用来生成包括 SOAP Web 服务及 Flash 远程服务在内的远程服务。它也可以作为 Adobe Flex 应用的后台服务器。

对此，360CERT 建议广大用户及时将 Adobe ColdFusion 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 漏洞详情

CVE-2021-21087: 远程代码执行漏洞

组件: ColdFusion

漏洞类型: 远程代码执行

影响: 接管服务器

简述: 未经授权的攻击者向 ColdFusion 服务器发送精心构造的恶意请求，在远程的服务器上执行任意代码，从而控制远程服务器。

五、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-21087	命令执行		严重

六、 安全建议

(一) 通用修补方案

- Adobe ColdFusion 2021：更新到 Adobe ColdFusion 2021 Update 1

- Adobe ColdFusion 2018：更新到 Adobe ColdFusion 2018 Update 11

- Adobe ColdFusion 2016：更新到 Adobe ColdFusion 2016 Update 17

注意：对于 ColdFusion 2016 HF7 及之前的版本，需要将 ColdFusion 的 JDK/JRE 更新到最新的版本。如果不更新 JDK/JRE，仅安装更新无法保护 ColdFusion 服务器的安全。

在 JEE 安装过程中，设置 JVM 标志：

-
Djdk.serialFilter= !org.mozilla.**;!com.sun.syndication.**;!org.apache.commons.beanutils.**

根据使用的应用程序服务器的类型，其启动文件可能不同：

- Tomcat：在 Catalina.bat/sh 文件中编辑 JAVA_OPTS

- Weblogic：在 startWeblogic.cmd 文件中编辑 JAVA_OPTIONS

- WildFly/EAP：在 standalone.conf 文件中编辑 JAVA_OPTS

七、 参考链接

1. https://helpx.adobe.com/security/products/coldfusion/apsb21-16.html

   https://helpx.adobe.com/security/products/coldfusion/apsb21-16.html

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危